Resource Sharing Alliance NFP
715 Sabrina Drive
East Peoria, IL 61611
866-940-4083

Personally Identifiable Information (PII) Protection Agreement for Libraries Who have Staff Accessing Advanced Reports in BLUEcloud Analytics

Last updated: March 21, 2024

RSA NPF and RSA Member Libraries are obligated to protect users' Personally Identifiable Information (PII) as a part of our professional ethics, in addition to our obligations under state and federal laws. BLUEcloud Analytics (BCA) is a powerful statistical analysis tool with a large amount of patron data including circulation activity and sensitive personal information. While PII is available via WorkFlows on a patron-by-patron basis, BCA allows extraction PII data for large numbers of patrons in any library and requires additional security measures and reporting procedures.

This agreement lists some of the responsibilities the library accepts when a staff member is granted access to advanced reports containing PII. Each individual staff member will also sign a personal PII Protection Agreement with RSA.

Each library with one or more staff members granted access to advanced reports must sign an overall PII Protection Agreement. This agreement must be signed by an authorized agent of the library. Individual staff members are required to sign a personal agreement as part of the increased access to advanced reports with potential PII data.

This Library agreement must be signed and returned to RSA before any staff gain advanced access. The signer is responsible for disseminating these terms to their library's staff.

Staff members who received BCA training prior to 1 Nov 2019 have already attended the advanced training. If these staff members have the need to access PII data, please notify RSA and we will work with them to get an individual agreement signed and their access upgraded.

Your Library agrees to:

- Limit the number of staff seeking Advanced Reports/PII access to only those who require access to this information. One employee can run reports for the entire library in most cases.
- Protect the security of BLUEcloud Analytics accounts, including not saving passwords to the shared password files or in non-password protected browser password tools.
- Not share BCA accounts or passwords between library staff.
- Avoid exporting or printing out unnecessary patron information and safeguard any data exported via files, emails, or printouts.

- Only use this information for library purposes. Accessing this information for non-library usage is prohibited.
- If we suspect a breach or misuse of BCA, we will notify RSA immediately.
- We agree to notify RSA, by phone or email within 24 hours, when a staff member with any level of BLUEcloud Analytics access leave the employment of the library for any reason so their account can be deactivated.
- We agree to notify RSA immediately by phone (within 4 hours) for any employee's non-consensual termination. These employees may hold a grudge and we need to immediately revoke their access to all RSA products and services.

Failure to do any of the above may result in advanced access being revoked for all staff members at your library.

_____ _____

Signature Printed Name

_____ _____

Library Date